

What is claimed is:

1 1. A method of processing and storing data in a
2 computer system including processor circuitry, and a data
3 storage device, the method comprising the steps of:

4 storing first and second sets of records on the
5 data storage device, the first and second sets of records
6 being of different data resolutions and corresponding to
7 overlapping periods of time;

8 operating the processor circuitry to receive
9 data collected over a period of time; and

10 operating the processor circuitry to update at
11 least one record in each of the stored first and second
12 sets of records with the received data.

1 2. The method of claim 1,

2 wherein the first and second sets of records
3 are stored in separate first-in, first-out data
4 structures on the data storage device; and

5 wherein the step of operating the processor
6 circuitry to update at least one record in each of the
7 stored first and second sets of records, includes the
8 step of replacing a previous record included in each of
9 the first and second data structures.

1 3. The method of claim 2, further comprising the step
2 of:

3 allocating fixed amounts of storage space on
4 the data storage device for storing each one of the first
5 and second first-in, first-out data structures used to
6 store the first and second sets of records.

1 4. The method of claim 2, wherein the first set of
2 records include hourly records and the second set of
3 records includes daily records.

1 5. The method of claim 2, further comprising the step
2 of:
3 periodically collecting network traffic data;
4 storing the collected network traffic data in a
5 buffer; and
6 operating the processor circuitry to retrieve
7 network traffic data from the buffer, the retrieved
8 network traffic data being received by the processor
9 circuitry.

1 6. The method of claim 5,
2 wherein the network traffic data stored in the
3 buffer includes time stamp information indicating the
4 period of time in which the network traffic data was
5 collected; and
6 wherein the step of operating the processor
7 circuitry to update at least one record in each of the
8 stored first and second sets of records includes the step
9 of:
10 examining at least one time stamp included in
11 the buffered network traffic data.

1 7. The method of claim 5, wherein the collected network
2 traffic data includes byte and packet count information
3 associated with each of a plurality of monitored
4 conversations between devices included in the computer
5 system, the step of operating the processor circuitry to

6 update at least one record in each of the stored first
7 and second sets of records including the steps of:
8 updating a record corresponding to a first
9 conversation in the first set of records; and
10 updating a record corresponding to the first
11 conversation the second set of records.

1 8. The method of claim 5,
2 wherein the processor circuitry includes first
3 and second central processing units, and
4 wherein the step of operating the processor
5 circuitry to update at least one record in each of the
6 stored first and second sets of records includes the step
7 of operating the first processor to update the first set
8 of records while operating the second processor to update
9 the second set of records.

1 9. The method of claim 1,
2 wherein the processor circuitry includes first
3 and second central processing units, and
4 wherein the step of operating the processor
5 circuitry to update at least one record in each of the
6 stored first and second sets of records includes the step
7 of operating the first processor to update the first set
8 of records while operating the second processor to update
9 the second set of records.

1 10. The method of claim 5, wherein the computer system
2 further includes a display device, the method further
3 comprising the step of:

7 the step of generating a database including the step of
8 generating from the information on each different
9 monitored conversation, a different record in each set of
10 the plurality of network traffic data sets.

1 15. The method of claim 14, further comprising the step
2 of storing each of the plurality of network traffic data
3 sets in a different first-in, first-out data structure.

1 16. The method of claim 15, wherein a limited amount of
2 data storage space is used for each of the different
3 first-in, first out data structures, the method further
4 comprising the step of:

5 overwriting the oldest data records in the
6 first-in, first-out data structure used to store one of
7 the network traffic data sets, when the limited amount of
8 data storage space used for said first-in, first-out data
9 structure is filled with records.

1 17. A system for monitoring network traffic data,
2 comprising:

3 a plurality of network traffic data probes for
4 collecting network traffic information;

5 processor circuitry coupled to the network
6 traffic probes for receiving data therefrom; and

7 a data storage device for storing a network
8 traffic database generated by the processor circuitry
9 using data collected by the network traffic data probes,
10 the data storage device including:

11 a plurality of data structures, each one of the
12 plurality of data structures including network traffic
13 data:

14 a) stored at a different resolution than the
15 resolution at which network traffic data is stored
16 in the other ones of the plurality of data
17 structures; and

18 b) corresponding to a period of time which
19 overlaps the period of time for which network
20 traffic data is stored in the other ones of the
21 plurality of data structures.

1 18. The system of claim 17, wherein each of the
2 plurality of data structures is a first-in, first-out
3 data structure.

1 19. The system of claim 18, wherein each one of the
2 plurality of data structures includes a plurality of data
3 records, each data record corresponding to a monitored
4 network conversation.

1 20. The system of claim 18, wherein data records are
2 arranged within each individual data structure as a
3 function of the time the conversation to which the record
4 corresponds was monitored.

1 21. The system of claim 20, wherein records which were
2 monitored during the same time interval are grouped
3 together within each individual data structure.

1 22. The system of claim 21, further comprising:

2 means for modifying at least one network
3 traffic data record included in each one of the plurality
4 of data structures to reflect collected information about
5 an individual network conversation.

1 23. The system of claim 18, further comprising:

2 means for modifying at least one network
3 traffic data record included in each one of the plurality
4 of data structures to reflect collected information about
5 an individual network conversation.

1 24. The system of claim 18, wherein the processor
2 circuitry includes a plurality of separate central
3 processing units which operate in parallel.

1 25. The system of claim 24, wherein each one of the
2 plurality of data structures includes a plurality of data
3 records, each data record corresponding to a monitored
4 network conversation.

1 26. The system of claim 24, wherein data records are
2 arranged within each individual data structure as a
3 function of the time the conversation to which the record
4 corresponds was monitored.

1 27. The system of claim 26, wherein records which were
2 monitored during the same time interval are grouped
3 together within each individual data structure.

